Defend what you create

User Manual

© Doctor Web, 2014. All rights reserved

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, Dr.Web AV-Desk and the Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web anti-virus for Android
Version 9.01.6
User Manual
14.10.2014

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Chapter 1. Introduction 6

Document Conventions 6

Main Features 7

Chapter 2. Licensing 8

License Key File 9

Acquire the Key File 9

Use License Key file 10

Update License 12

Chapter 3. Installation 13

System Requirements 13

Install Program 13

Update and Uninstall Program 14

Chapter 4. Start to Use 16

Launch and Exit Program 16

Interface 16

Widgets 18

Notifications 18

My Dr.Web 19

Chapter 5. Application Functions 20

Anti-Virus Protection 21

Constant Anti-Virus Protection 21

On-Demand Scan 22

Threats Neutralization 24

Threats Detection in System Applications 24

Processing Device Lockers 25

Calls and SMS Filter 25

Filtering Mode 26

Black List 26

Create Filtering Profile 27

View Blocked Calls and SMS 28

Update 28

Quarantine 29

Statistics 31

Dr.Web Anti-theft 32
Configure General Settings 32
Additional Functions 34
Buddies List 35
SMS Commands 36
Unlock the Device and Reset Password 37
Restricting Internet Access 37
Dr.Web Firewall 38
Limit the Use of Mobile Internet 40
Processing Applications Traffic 41
Current Internet Activity 43
Logging 43
Security Troubleshooting 45
Operation Mode 47
URL Shortening Service 49
Appendices 50
Appendix A. Technical Support 50
Index 51

Chapter 1. Introduction

Thank you for choosing **Dr.Web anti-virus for Android** (hereinafter referred to as **Dr.Web anti-virus**). This anti-virus solution offers a reliable protection of the mobile phones and communicators working under the Android™ operating system from various virus threats designed specifically for mobile devices.

The program employs the most advanced developments and technologies of **Doctor Web** aimed at detection and neutralization of malicious objects which may represent a threat to the device operation and information security.

Dr.Web anti-virus uses Origins Tracing™ for Android — the unique algorithm to detect malware designed specially for Android. This algorithm allows detecting the new virus families using the knowledge database on previous threats. Origins Tracing for Android can identify the recompiled viruses, e.g. Android.SMSSend, Android.MobileSpy, as well as the applications infected by Android.ADRD, Android.Geinimi, Android.DreamExploid. The names of the threats detected using Origins Tracing for Android are Android.VirusName.origin.

This manual is intended to help users of mobile devices to install and adjust **Dr.Web anti-virus**. It also describes all the basic functions of the application.

Document Conventions

The following conventions and symbols are used in this document:

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of Dr.Web products and components.
Green and underlined	Hyperlinks to topics and webpages.
Italic	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
	A warning about potential errors or any other important comment.

Main Features

Dr.Web anti-virus is a reliable anti-virus solution for users of mobile devices working under the Android operating system. The application protects devices from information security threats and spam by performing the following functions:

- Constant real-time protection of the file system (scanning of saved files, programs which are being installed etc).
- Scanning of the whole file system of the device or files and folders selected by user
- Scanning of the archives
- Scanning of the files on removable memory cards
- Detection of Windows autorun files
- Threats detection in the .lnk files (defined by **Dr.Web** as **Exploit.CplInk**)
- Deletion of the infected objects or their isolation in quarantine
- Device unlocking if it is locked by ransomware
- Filtering the unsolicited calls and SMS using the predefined and custom black and white lists settings
- **Dr.Web virus databases** updates via Internet
- Statistics of the detected threats and performed actions, program log
- Detecting the device location or locking its functions in case it has been lost or stolen
- Restricting access to the undesirable Internet resources when using the default Android browser, Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser or Boat Browser Mini
- Scanning and shortening URLs
- Controlling the Internet connections, protecting your device from unauthorized access and preventing leak of vital data through networks
- Analyzing the security of the device and help in resolving the detected problems and vulnerabilities

Dr.Web anti-virus has user-friendly interface and easy customizable settings which help you configure all program options to set up the appropriate protection level.

Dr.Web anti-virus also supports working in Multi-Window mode that allows you to launch several applications in separate windows. This mode can be used only on Samsung Galaxy S III or higher version and Samsung Galaxy Note 2 or higher version.

Chapter 2. Licensing

The *key file* regulates the use rights for the purchased product.

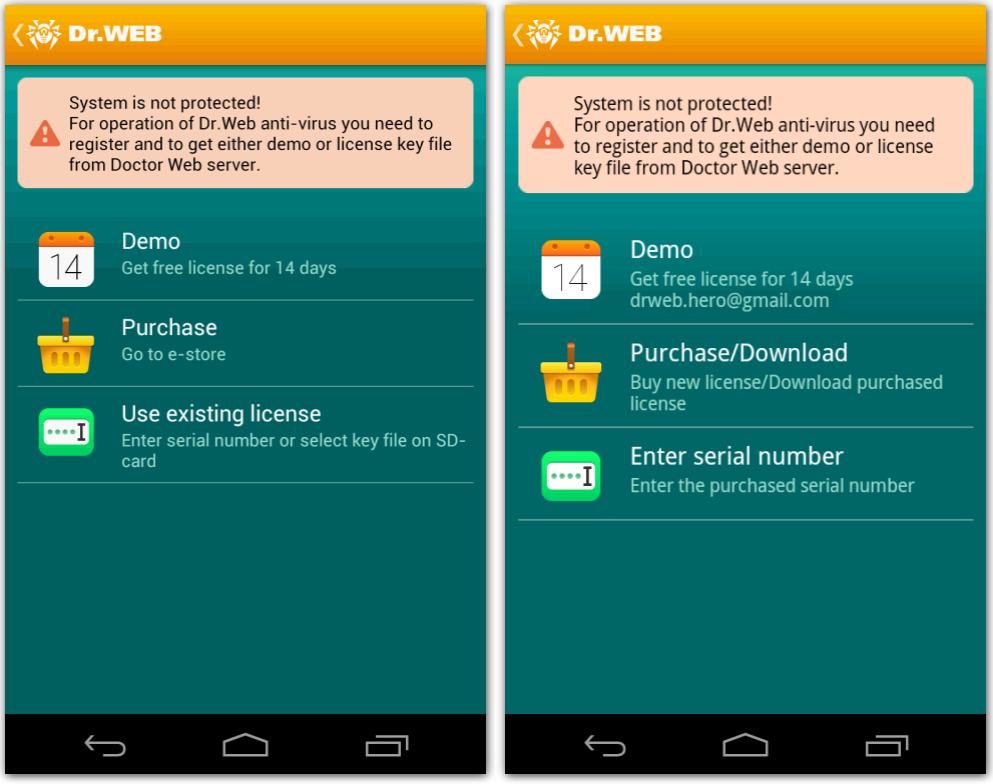
The purchase and registration procedure is different for the **Dr.Web anti-virus** version available for installation in Google Play and the one downloaded and installed from the **Doctor Web** website.

In case you purchase the application version with the unlimited license (**Dr.Web Anti-virus Life license**) from Google Play, the license key file is received and registered automatically.

When central protection mode is activated, the license is automatically downloaded from the central protection server.

If you have the license for the products **Dr.Web® Security Space** or **Dr.Web® Desktop Security Suite** or any packaged **Dr.Web** product, you can use the existing license key file for operation of **Dr.Web anti-virus**.

To get or register the license, use the corresponding screen (see Figures 1a, 1b). This screen opens on the first launch of the program and in case license key file is missing. You can also open this screen by opening the application menu on the main screen of the program (see Figure 2) and tapping **About** -> **Renew license**.


Dr.WEB
System is not protected!
For operation of Dr.Web anti-virus you need to register and to get either demo or license key file from Doctor Web server.
Demo
Get free license for 14 days
Purchase
Go to e-store
Use existing license
Enter serial number or select key file on SD-card
Dr.WEB
System is not protected!
For operation of Dr.Web anti-virus you need to register and to get either demo or license key file from Doctor Web server.
Demo
Get free license for 14 days
drweb.hero@gmail.com
Purchase/Download
Buy new license/Download purchased license
Enter serial number
Enter the purchased serial number

Figures 1a and 1b. Licensing

License Key File

A key file contains, among other, the following information:

- Licensed period for the product
- List of components the user is allowed to use
- Other limitations

There are two types of key files:

- *License key file* is purchased with the **Dr.Web anti-virus** and allows purchasers to use the software and receive technical support. Parameters of the license key file are set in accordance with the software's license agreement. The file also contains information about the purchaser and seller.
- *Demo key file* is used for evaluation of **Dr.Web** products. It is distributed free of change and provides full functionality of the software. However demo key files have limited validity period.

A *valid* license key file satisfies the following criteria:

- License is not expired.
- The license applies to all components of the product.
- Integrity of the license key file is not violated.

If any of the conditions are violated, the license key file becomes invalid, **Dr.Web anti-virus** stops detecting and neutralizing the malicious programs.

The license key file becomes invalid after editing. Do not save changes after opening the file in text editors to prevent the license from compromise.

Acquire the Key File

Get demo key file

If you installed the program in purposes of evaluation, you can download the free license for 14 days. To do this, tap **Demo** on the licensing screen (see Figures 1a, 1b):

- If you installed the application from Google Play, the key file is registered on the email address of your Google account shown in the **Demo** section. If you have several Google accounts, the first of them will be selected for registering the key file. If you do not have a Google account, enter a valid email address to register the license.
- If you request a demo key file for the application version downloaded from the **Doctor Web** website, you need to fill in the registration form. Enter your personal data required for demo key file download and tap **Get license**.

The key file will be downloaded and installed automatically. On completing the download, the information on the received key file and its validity period will be displayed on the screen.

Purchase license and get license key file

Depending on the installation type of the application, the following procedures to acquire the license for **Dr.Web anti-virus** are available:

1. If you installed the application via Google Play, on the licensing screen (see Figure 1b), select **Purchase/Download**. Enter your email address to register the license key file. This will allow you to download the purchased key file to use with **Dr.Web anti-virus** in case you re-install the application or install it on another device. On the **Purchase license** screen, select one of the license types:
   - **1 year license**, **2 year license** or **1 year license without technical support**. If you select one of these license types, the standard application purchase window will open. The corresponding license key file will be downloaded on your device in some time after completing the payment. Once the download completes, the information on the license and its validity period will be displayed on the screen. If the download did not start because of a technical issue, please contact the **Doctor Web** technical support.
   - **Unlimited license**. If you select the license without any time limits, you'll be brought to the **Dr.Web anti-virus Life license** product purchase and installation in Google Play. If you used **Dr.Web anti-virus**, you'll be asked to delete it. Tap **OK** to confirm the removal. If you want to save application settings in order to use them with **Dr.Web anti-virus Life license**, export the current configuration to file before deleting the application.

   If you have **Dr.Web Anti-theft** enabled on your device, clear the **Dr.Web anti-virus** check box on the **Location and Security** tab of the **Select device administrator** section in the device settings before uninstalling **Dr.Web anti-virus** (the names of settings can be different depending on the device model and operating system version). Your device will be locked by **Dr.Web Anti-theft**. Enter the password set for **Dr.Web Anti-theft** to continue the application removal.

   The license key file will be downloaded and installed automatically during the installation of **Dr.Web anti-virus Life license**.

2. If you installed the application from the **Doctor Web** website, you can purchase the license for **Dr.Web anti-virus** in the **Doctor Web** web store by tapping **Purchase** on the licensing screen (see Figure 1a) or by opening the URL http://estore.drweb.com/mobile. Select the license period and the number of mobile devices to protect, then click **Buy**. You will receive either the serial number or the license key file to the email specified while ordering. You can also choose to receive the serial number in an SMS to the mobile number entered on registration. To start using the purchased license you need either to register the serial number or copy the key file on the device.

Use License Key file

If you already have a key file for **Dr.Web anti-virus** or you have the license for **Dr.Web Security Space**, **Dr.Web Desktop Security Suite** or any packaged **Dr.Web** product, you can register and use the existing license in the following ways, depending on the method of the **Dr.Web anti-virus** installation on your device:

1. If you installed **Dr.Web anti-virus** via Google Play and already requested and received either demo or license key file, on the **Dr.Web - License** screen (see Figures 1a, 1b), tap **Purchase/ Download**. Enter the email address that you have previously used to get/register the key file, if necessary. The license registered on the specified email address will be restored automatically from the server. If you have the serial number, you can use it to download the license key file to your device via Internet.
2. If you installed **Dr.Web anti-virus** from the **Doctor Web** website, you can either copy the existing key file to a special folder on the SD card or register the existing serial number in order to get the license key file by email or download it to your mobile device via Internet.

The key file for **Dr.Web Security Space** or **Dr.Web Desktop Security Suite** program can be used with **Dr.Web anti-virus** only if it supports DrWebGUI component.

To check whether such key file can be used:

1. Open the key file in a text editor (e.g., Notepad).
2. Check the list of values of the Applications parameter in the [Key] group: if DrWebGUI component is in the list, you can use the key file for operation of **Dr.Web anti-virus**.

The key file is secured with digital signature. Do not edit or otherwise modify the file to prevent the license from compromise.

Copy key file on the device with Dr.Web anti-virus

1. Synchronize your device with PC and copy the key file to the **Android/data/com.drweb/files** folder located on the SD card.
2. On the licensing screen (see Figures 1a, 1b) select **Use existing license**.
3. Tap **Copy from file**. On the information window **Copy from file** tap **OK**.
4. The key file will be downloaded and installed. Review the license expiration date in the information window. Tap **OK**.

Get license key file by registering serial number

You can get the key file by email after the product registration on **Doctor Web** official website. To do this:

1. Launch an Internet browser and go to the site which is specified on the product registration card supplied with your copy of the product.
2. Enter the serial number which is typed on the registration card.
3. Fill in the registration form.
4. The license key file is archived and sent to the email address you specified in the registration form.
5. Extract the license key file on the computer that will be used for synchronization with your device and copying the key file.

You can also download the key file directly to the device via Internet. To do this:

1. On the licensing screen (see Figure 1a) tap **Use existing license**.
2. Tap **Enter serial number**.

The serial number received to activate the demonstration period of **Dr.Web** product for workstations cannot be used with **Dr.Web anti-virus** version installed from Google Play. You need to activate the demo period for the corresponding **Dr.Web** product on PC at first, so that you will get the license key file. then you can copy it to the mobile device. The instructions on using the received license key file on mobile devices will be sent to you by email during the demonstration period activation.

3. Enter the serial number and tap **Get license**.
4. If you're registering this serial number for the first time, you will be asked to enter your personal data. This information is necessary to receive the key file. After you fill in all the fields, tap **Get license**.
5. The key file will be downloaded and installed. The key file downloading procedure log is displayed on the screen:
   - If the license key is downloaded successfully, tap **OK**.
   - If an error occurred, the error details are displayed.

Update License

When license expires, you may need to update the license. The new license then should be registered with the product or the expired license should be renewed if it is supported for your key file. **Dr.Web anti-virus** supports hot license update without stopping or reinstalling the program.

Get information on license

1. On the main screen (see Figure 2) open the application menu and tap **About**.
2. You can review the following information on the licensing parameters on the :
   - License owner name
   - License activation and expiration dates

Configure notifications

You can enable/disable notifications about the upcoming license expiration using the **Notifications** option on the **License** section in **Dr.Web anti-virus** settings (see Figure 6).

Update license

To update your license, you need either acquire or register the new key file.

You can also purchase a new license or renew your current license on your personal web page at **Doctor Web** official website. To go to this web page, tap **About** in the application menu and click the **My Dr.Web** link.

Chapter 3. Installation

Dr.Web anti-virus can be purchased and installed on the mobile device directly from Google Play or by launching the installation file **drweb-901-android.apk**. You can also install the application using the synchronization with PC.

The program can be removed via Google Play or by means of the operational system of the device.

System Requirements

To install and use **Dr.Web anti-virus**, ensure your mobile device works under the Android operating system of 2.1/2.2/2.3/3.0/3.1/3.2/4.0/4.1/4.2/4.3/4.4 version.

The Internet connection is also required for virus databases update procedure. If you are using a tablet, for correct operation of calls and SMS filtering and **Dr.Web Anti-theft**, it is required to support the use of SIM cards. **Dr.Web Firewall** is available only on the devices running Android 4.0 or higher.

Please note that the correct operation of **Dr.Web anti-virus** is not guaranteed on the devices with custom ROMs and on the "rooted" devices! Technical support is not also provided for such devices.

Install Program

You can install **Dr.Web anti-virus** either via Google Play or launch the program installation file on the device or via synchronization with PC.

Installation via Google Play

1. Open Google Play, find **Doctor Web** in the list of applications and tap **Install** **Purchase** depending on the type of the application you would like to install.

   If your mobile device does not meet the system requirements, **Dr.Web anti-virus** is not displayed in the list of Google Play.

2. If you are installing the application version with the unlimited license (**Dr.Web anti-virus Life license**), the screen with payment options will open.
3. After completing the payment, on the screen with information on the application review the required access rights. The program requires access to the following data:
   - If you're installing **Dr.Web anti-virus** free trial for 14 days, access to the in-app purchases function is required for further license purchase.
   - For application registration and license activation, Internet access and access to the list of Google accounts of the device are required.
   - For operation of **SpIDer Guard** file monitor and scanner, access to device memory, SD card and applications data, as well as reading/writing permissions are required.
   - For calls and SMS filtering, access to calls and SMS receiving/sending function, permissions for reading contact list, calls and messages logs and changing signals (to turn off sound if the call is blocked) are required.

- For **Dr.Web Anti-theft** operation, permissions for sending SMS (to send **Dr.Web Anti-theft** messages about changing SIM card and replies to received commands), getting device coordinates, GPS and Wi-Fi managing and deleting all personal information from the device (in case a corresponding command is received) are required.
- For **Cloud Checker** URL filter operation, access to browsing history and bookmarks of the supported browsers is required.
- For updating virus databases, access to Internet and device network settings is required.

Tap **OK**.

4. The application will be installed automatically.

For program installation without Google Play, you need to allow it on your device. To do this, select the **Unknown sources** check box on the **Settings** -> **Applications** screen. The installation file of **Dr.Web anti-virus** is available for download on the **Doctor Web** website at http://download.drweb.com/android.

Installation via launching the drweb-901-android.apk file directly on the device

1. Copy the installation file **drweb-901-android.apk** to the SD card.

To launch the installation file on the device a file manager is required.

2. Use the file manager to find and launch the installation file.
3. The application will be installed automatically.

Installation via device synchronization with PC using special synchronization software (e.g., HTC Sync™ etc.)

1. Synchronize your device with the PC.
2. Launch the installation manager included into the synchronization software package.
3. Specify the path to the file **drweb-901-android.apk** located on the computer, then follow the instructions of the installation wizard.
4. The application will be copied to the device where you can review the information on it and confirm the installation.
5. Close the installation wizard.

Dr.Web anti-virus was successfully installed on your device and is ready to use. In case you have installed the program without Google Play, you need to register the license for further operation of the application. If you do not have a valid key file, you can acquire it.

By default, the application is installed to the device memory. For correct operation of **Dr.Web Anti-theft** function, do not transfer the installed application to removable media.

Update and Uninstall Program

The program can be updated or uninstalled via Google Play. You can also uninstall the program by means of the operating system connecting to Internet.

In case **Dr.Web Anti-theft** is enabled on your device, you need to clear the **Dr.Web anti-virus** check box on the **Location and Security** tab of the **Select device administrator** section in device settings before uninstalling the application (the names of settings can be different depending on the device model and the operating system version).

Update or uninstall program via Google Play

1. Open Google Play and select **Downloads** or **My Android Apps** (depending on the version of the operating system).
2. Tap the sign of **Dr.Web anti-virus** in the list of downloaded applications.

If **Dr.Web anti-virus** was installed without Google Play, it would not be shown in the **Downloads** section. In this case you can delete it by means of the operating system.

3. On the screen with the information on the application tap **Update** or **Uninstall**.
4. Confirm the program update/removal:
   - In case you are updating the program, the next steps are similar to the ones described in the Install Program section.
   - In case you are uninstalling the program, specify the reason of the program removal and tap **OK**. The program will be removed from the device.

Uninstall program without connecting to Internet

1. Open the **Settings** -> **Applications** -> **Manage applications** screen.
2. Tap the **Dr.Web anti-virus** sign in the list of installed applications.
3. On the screen with the information on the application tap **Uninstall**. The program will be removed from the device.
4. Tap **OK** to return to the list of the installed applications.

Quarantine and saved program log are not deleted by default. You can delete them manually from the Android/data/com.drweb/files folder on the SD card.

Check the availability of the new version of application

If you downloaded and installed **Dr.Web anti-virus** from **Doctor Web** website, you can enable check for the new version availability every time the virus databases are updated. To do this, select the **New version of app** check box in the application update settings section. When a new version of the application becomes available, you will get a standard notification to download and install it.

Chapter 4. Start to Use

This section describes the interface of **Dr.Web anti-virus** and provides step-by-step procedures for launching or exiting the application.

Launch and Exit Program

To launch the application

To launch **Dr.Web anti-virus**, open the **All programs** screen and tap **Dr.Web anti-virus** sign . On the first launch of the program you will be asked to read and accept the License agreement, that is necessary to start using the application. In the same window, you may also agree to participate in the software quality improvement program by allowing to send impersonal data about the detected threats and visited websites to **Doctor Web** and Google servers. You can disable sending such statistical information at any time by clearing the **Sending statistics** check box in the **General settings** section of the application parameters.

To exit the application

To exit **Dr.Web anti-virus** press the **Home** button.

You can use the **Dr.Web anti-virus** sign in the recently launched programs section to activate the application from the background operation.

When you first launch **Dr.Web anti-virus**, the application opens on its main screen. When you activate the application from the background operation, the application opens on the last active screen.

Interface

On the program main screen (see Figure 2) the current protection status is displayed. It also provides access to the following program functions:

- **SpIDer Guard** – allows to enable/disable the constant anti-virus protection.
- **Calls and SMS filtering** – allows to specify the filtering mode and review the lists of blocked calls and messages.

> If you are using a tablet without SIM cards support, the calls and SMS filtering is not available, so the corresponding section will be absent on the main application screen.

- **Scanner** – provides the on-demand scanning of the system (3 scan types are possible: full scan, quick scan and custom scan).
- **Update** – contains information on the date of the last update and launches the program update if required.
- **Anti-theft** – allows to configure **Dr.Web Anti-theft**.
- **Cloud Checker** – allows to configure the URL-filter to restrict user access to the Internet ressources.
- **Firewall** – allows to configure control of the Internet connections and data transfer over the network.
- **Security Auditor** – allows to perform the diagnostics of the system and helps to resolve the detected security problems and vulnerabilities.

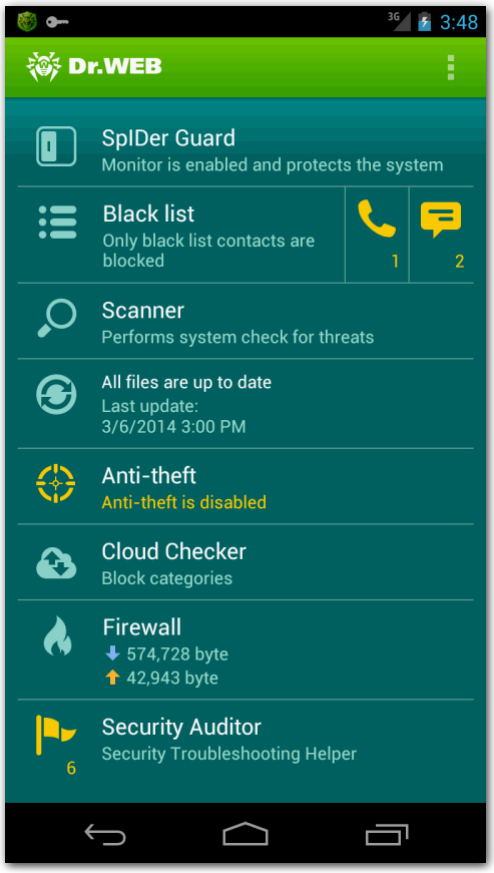


Figure 2. Main screen of the program

Accessing the application menu and navigating between screens

To open the application menu with additional options, tap the corresponding item in the upper right side of the screen. To return to the previous screen, tap the application logo in the upper left side of the screen.

The application menu on the main screen allows you to open the program settings, to access quarantine and application statistics, as well as open the program information screen.

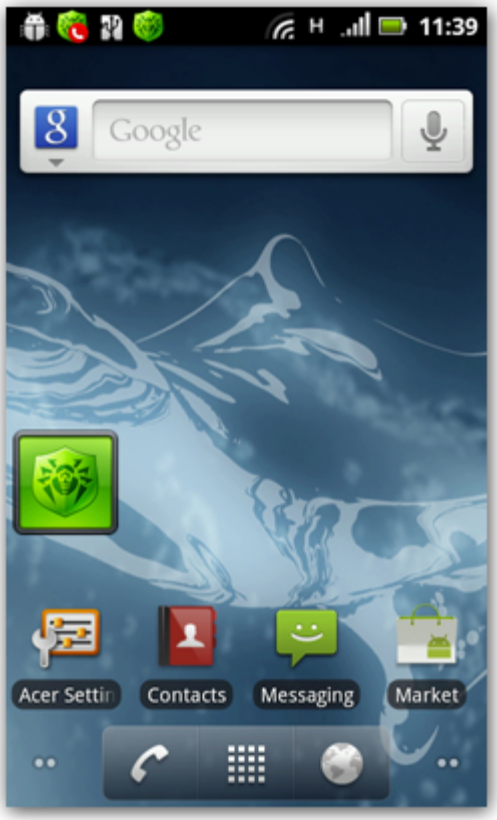
The program information screen contains information on the application version, the number of entries in **Dr.Web virus databases**, the license owner and its activation and expiration dates. It also contains links to **Doctor Web** official website, your personal web page there and to the pages of the company in social networks: Twitter, Facebook, Instagram, and to its Youtube channel. If **Dr.Web anti-virus** is operating in central protection mode and is used to connect to **Dr.Web® AV-Desk** anti-virus service, the screen also contains the subscription expiration date or the date when the service was blocked for the device (station).

Widgets

To make the work with **Dr.Web anti-virus** easier and more convenient, you can add on your device **Home Screen** the special widgets which allow to manage the main program functions.

To add widget

1. Open the list of available widgets using the standard widget adding feature of your device.
2. Select one of **Dr.Web anti-virus** widgets in the list:
   - **Dr.Web 1x1 (small)** – displays the current protection status and allows to enable/disable the monitor **SpIDer Guard** (see Figure 3).
   - **Dr.Web 4x1 (medium)** – displays the current protection status, the selected filtering profile, the number of blocked calls and messages and allows to enable/disable the monitor **SpIDer Guard**, open the scanner screen (see Figure 4).



Figures 3 and 4. Dr.Web widgets

Notifications

Dr.Web anti-virus features a special pane in the notifications area on the device screen providing a quick access to the main application functions (see Figure 5). You can enable/disable this type of notifications using the **Notifications pane** option on the **General settings** section (see Figure 6).

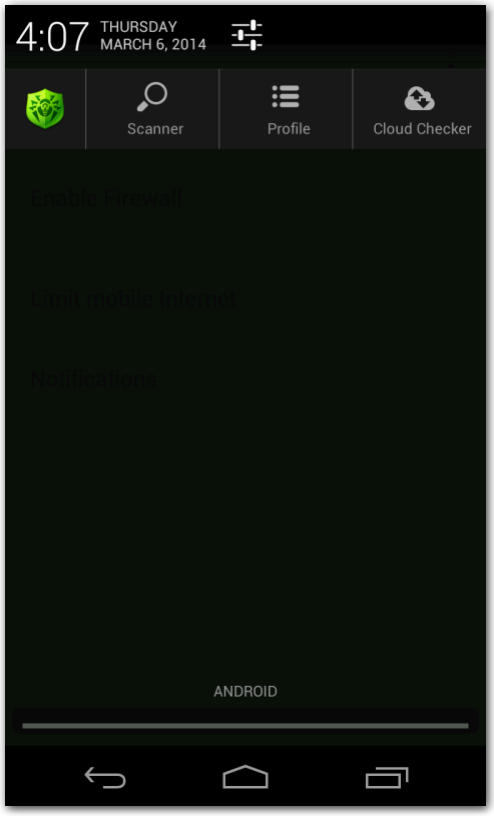


Figure 5. Notifications pane

This pane allows you to perform the following actions:

- Open the **Dr.Web anti-virus** screen. To do this, tap the **Dr.Web** icon.
- Launch quick, full or custom scan by tapping **Scanner** and then selecting the scan type.
- Select the calls and SMS filtering profile by tapping **Profile**.

If your device does not support the use of SIM cards, the notifications pane contains the **Downloads** option allowing to launch the downloads scan instead of the **Profile** one.

- Open the URL filter configuration screen by tapping **Cloud Checker**.

In case threats are detected, the icons in the notifications pane change to indicate it:

- – if the threats are detected by scanner.
- – if the threats are detected by file monitor **SpIDer Guard**.

My Dr.Web

Online service **My Dr.Web** is your personal web page of the official **Doctor Web** website. This page provides you with information on your license including usage period and serial number, allows to renew the license, review the information on the last update and the number of records in virus databases, contact Technical Support, etc.

To open this page, on the main screen (see Figure 2) open the application menu and tap **About**. Then tap **My Dr.Web** on the opened screen.

Chapter 5. Application Functions

This section describes main features of **Dr.Web anti-virus** and provides step-by-step procedures of setting up the anti-virus check, SMS and calls filtering, the operation of **Dr.Web Anti-theft** and URL filter for configuring protection of your device.

To open the settings screen (see Figure 6), on the main screen open the application menu and select **Settings**.

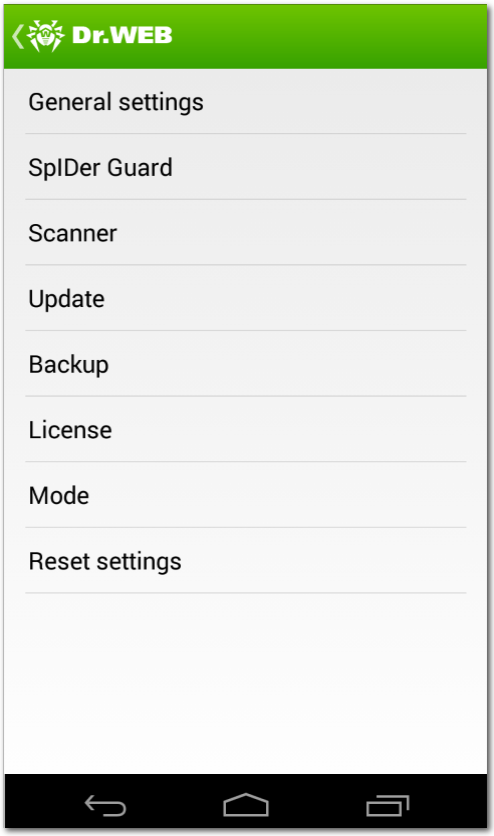


Figure 6. Application settings

Reset settings

You can reset the user settings of the application at any time and restore the standard settings. To do this:

1. Tap **Reset settings** on the settings screen (see Figure 6). On the opened screen, tap **Restore default settings** item.
2. Confirm the return to the default settings.

Import and export settings

You can also save all current application settings to the file on the SD-card. You will be able to re-use them in future (for example, in case you re-install **Dr.Web anti-virus** or use it on another device) by downloading from the file.

1. To save the current configuration, on the settings screen (see Figure 6) tap **Backup** and then tap **Export data**. In the **Export data** window enter the password to set up for protection of the settings file, then tap **OK**. All settings are saved in the Android/data/com.drweb/files/DrWebPro.bkp file on the SD-card.

2. To load the saved settings from the file, on the settings screen (see Figure 6) tap **Backup** and then tap **Import data**. Confirm the settings and parameters loading from the file and enter the password of file. All current application settings will be replaced by the settings from the file.

Anti-Virus Protection

The main function implemented in **Dr.Web anti-virus** is the ability to constantly scan the file system in real-time mode. **Dr.Web anti-virus** also performs system on-demand scans. On security threats detection, **Dr.Web anti-virus** performs actions selected by the user.

Constant Anti-Virus Protection

The constant system protection is carried out by a component **SpIDer Guard** called *file monitor*. It resides in the memory of the device and checks all files as they are modified and saved.

Enable constant protection

On the first launch of the program the constant protection is enabled automatically after you accept the License Agreement. To disable or re-enable it, tap the **SpIDer Guard** section of the main screen.

When monitor is enabled, it begins protecting the file system of the device. It remains active even if you close the application. If a security threat is detected, the alerting sign appears in the status bar on the screen as well as a popup window notifying about the threats detection. After opening the notifications panel you can review the information on the number of the detected threats and access to the list of the threats to choose actions for their neutralization.

File monitor stops when the device memory is cleared using the default Task Manager. To restore constant anti-virus protection, reopen **Dr.Web anti-virus**.

Monitor settings

To access the **Dr.Web anti-virus** settings, open the application menu on the main screen and tap **Settings**. To configure the monitor, perform the following actions on the settings screen (see Figure 6):

- To enable check of files in archives, select the **Files in archives** check box on the **SpIDer Guard** section.

By default, the archives check is disabled. Enabling the check of archives can influence the system performance and increase the battery power consumption. Anyway, disabling the archives check do not decrease the protection level because the monitor checks the Android installation files (.apk) regardless of the **Files in archives** parameter value.

- To enable check of the files on the SD card on each mounting, select the **SD card mounting** check box on the **SpIDer Guard** section.
- To enable/disable the detection of adware and riskware (including hacktools and jokes), tap **More options** on the **SpIDer Guard** section, then select/clear the **Adware** and **Riskware** check boxes.
- To enable the SD card check for Windows auto run files, select the **Autorun files** check box on the **General settings** section. This option configures the on-demand scans as well.
- To show the sign in the status bar on monitor activity, select the **Ongoing notifications** check box on the **General settings** section.

Statistics

Dr.Web anti-virus registers the events related to the monitor operation (enable/disable, SD card and installed applications check results, threats detection). The program actions are displayed on the **Actions** section of the **Statistics** screen.

On-Demand Scan

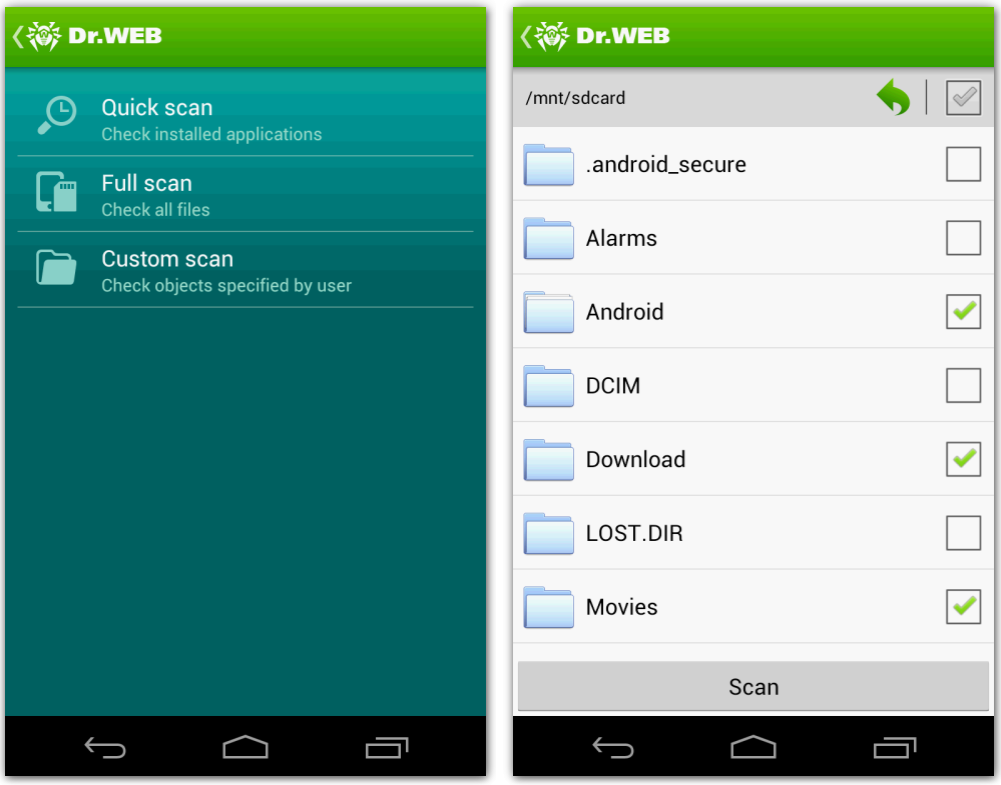
Dr.Web anti-virus provides on-demand scanning of the file system. You can perform quick or full check of the whole file system or scan the critical files and folders only. This function is performed by the **Dr.Web** *scanner*.

Scanning

To scan the system, on the main screen tap **Scanner** and on the opened screen (see Figure 7) do one of the following actions:

- To launch only the installed applications check, tap **Quick scan**.
- To scan all the files, tap **Full scan**.
- To scan only critical files and folders, tap **Custom scan**, select the objects in the hierarchical list (see Figure 8) and then tap **Scan**. While selecting the objects to scan, you can use the options located to the right above the list to select all objects and to go up one folder.

After the scanning completes, you can review the list of detected threats and choose an action for each malicious object.



Figures 7 and 8. Scanner and custom scan screens

Sending suspicious files to Doctor Web Laboratory

You can submit a suspicious file, presumably a virus, or a clean file that has been identified as so-called "false positive" to **Doctor Web** Laboratory:

1. Tap and hold the file in the hierarchical list (see Figure 8), then tap **Send to Laboratory**.
2. In the next screen, enter your email address in order to receive the results of the file analysis.
3. Select a category for your request:
   - **Suspicious file**, if you think that the file represents a threat.
   - **False detection** or **False detection by Origins Tracing**, if you think that the file was identified as threat by mistake.

   To make a selection between two categories of false detection, use the name of the threat that the file presumably contains: select the **False detection by Origins Tracing** category, if the name contains the ".origin" postfix and the **False detection** one in other cases.
4. Tap **Submit**.

Only the files of not more than 10 MB can be submitted to **Doctor Web** Laboratory.

Scanner settings

To access to the scanner settings, on the main screen open the application menu, tap **Settings** and select **Scanner** section.

- To enable check of files in archives, select the **Files in archives** check box on the **Scanner** section.

By default, the archives check is disabled. Enabling the check of archives may influence the system performance and increase the battery power consumption. Anyway, disabling the archives check does not decrease the protection level because the monitor checks all the Android installation files (.apk) regardless of the **Files in archives** parameter value.

- To show the paths to the scanned files for each processor core separately when using the multi-core devices, select the **Progress by cores** check box on the **Scanner** section.
- To enable/disable the detection of adware and riskware (including hacktools and jokes), tap **More options** on the **Scanner** section, then select/clear the **Adware** and **Riskware** check boxes.
- To enable the SD card check for Windows auto run files, select the **Autorun files** check box on the **General settings** section. This option configures the real-time scan as well.

It is strongly recommended to periodically scan the system in case the monitor had not been active for some time. Usually, the quick scan is sufficient for this purpose.

Statistics

Dr.Web anti-virus registers the events related to the scanner operation (check type and results, threats detection). The program actions are displayed on the **Actions** section of the **Statistics** screen.

Threats Neutralization

Viewing the list of detected threats

In case threats were detected by the file monitor **SpIDer Guard**, the sign appears in the status bar on the screen. A tooltip notifying about the threats detection is also displayed on the screen. Open the notifications panel and tap the message about the number of the detected threats to open the full list of malicious objects.

When scanning your device by scanner, the list of the detected threats opens automatically after the scan is completed.

For each threat in the list, the following information is displayed:

- Name of the threat
- Path to the file containing the threat

The type of threats that were not detected as viruses is displayed in brackets: adware, riskware, joke or hacktool program.

Performing actions over the threats

Tap the threat in the list to see the available actions and to apply one of them to the selected threat. **Dr.Web anti-virus** allows to choose one of the following actions for detected threats:

- **Delete** – the threat is completely removed from the device memory.
- **Move to quarantine** – the threat is moved to a special folder where it is isolated from the rest of the system.

If a threat is detected in an installed application, it cannot be moved to quarantine. In this case the **Move to quarantine** action is missing in the list of actions.

- **Ignore** – the threat is temporarily ignored and no action is applied to it.
- **Report false positive** – you can send the threat to **Doctor Web Anti-Virus Laboratory** to report that it is not harmful and was identified by the anti-virus as dangerous by mistake. Enter your email in order to receive the results of the file analysis. Tap **Send**.

The **Report false positive** action is available only for the threat modifications with ".origin" postfix.

You can set up sound notifications on threats detection, deletion or moving to quarantine. To do this, on the main screen open the application menu and tap **Settings**, then select the **Sounds** check box on the **General settings** section of the settings screen (see Figure 6).

Threats Detection in System Applications

Sometimes the system applications installed on your device by manufacturer can perform functions that are typical for malware. During the scanning by **Dr.Web anti-virus** such application are detected as security threats and a corresponding notification is prompted. The standard threats neutralization actions are not applicable to the system applications. However, you can use the following guidelines:

- Stop the application from the device settings (open the **Settings** -> **Applications** screen and tap the application detected as threat, then on the screen with information on this application, tap **Stop**).

This action needs to be redone every time the device is restarted.

- If a custom operating system (ROM) is installed on the device, you can restore the factory settings and use the official software of your device manufacturer.
- If you are using official software of the device manufacturer, try to contact the vendor for more information on this application.
- If your device is rooted, you can try to delete this application using special tools and utilities.

You can also disable the notifications about threats detection in known system applications using the **System applications** option on **General settings** -> **More options** section of the settings screen (see Figure 6).

Processing Device Lockers

Dr.Web anti-virus protects the mobile devices against ransomware programs targeting Android users that expanded markedly. These programs pose severe danger to Android smart phones and tablets. They can encrypt the files on memory cards, lock the device screen and display a ransom demand for the decryption of the files and unlock the device.

Photos, videos and documents stored on memory cards can be compromised by such malicious programs. In addition, they steal and transmit to the intruders' servers various information about the infected device (including, for example, its IMEI), information from the infected device's phone book (contact names, phone numbers and email addresses). Ransomware programs monitor incoming and outgoing communications and can bar those communications if desired. All the information collected, including phone call data, is also transmitted to the control server.

Dr.Web anti-virus detects and removes ransomware programs whenever they try to penetrate a protected device. However, they are characterized by the high-speed evolvement and modification. So, especially if **Dr.Web virus databases** have not been updated for some time and do not contain information on new examples, the device lockers can be installed on the device.

If your mobile device is locked by a ransomware program and **SpIDer Guard** is enabled on it, you can unlock your device by performing the following actions:

1. Connect your device to a charger.
2. In the next 5 seconds, unplug a charger.
3. In the next 10 seconds, shake your device briskly.
4. **Dr.Web anti-virus** ends all active processes on the device, including the one of the application locker, and then activates a vibration signal (on the devices which have this feature). Then **Dr.Web anti-virus** screen will open.

Please note that ending active processes can result in losing data of other applications that were active when the device was locked.

5. After the device is unlocked, it is recommended to update **Dr.Web virus databases** and perform a quick scan of the system, or to delete the malicious application from your device.

Calls and SMS Filter

Dr.Web anti-virus filters the incoming phone calls and SMS. It allows to block the undesired messages and calls, such as advertisements or messages and calls from unknown numbers.

The correct operation of SMS filtering is not guaranteed on Android 4.4.

The filtering mode is specified by user. The program provides you with the predefined profiles, which determine the filters. You can also create user profiles with separate filtering settings.

The information on the blocked calls and messages is available on the **Blocked calls and SMS** section.

Filtering Mode

You can chose one of the followings messages and calls filter types:

- **Accept all**. In this case filtering is disabled and all the incoming calls and SMS are accepted.
- **Reject all**. In this case all the incoming calls and SMS are blocked.
- **Phone book**. In this case calls and SMS only from the phone book contacts are accepted.
- **Black list**. This filter type means that the phone calls and SMS from the numbers included into the black list are blocked.

Alternatively, you can use the custom filter. **Dr.Web anti-virus** allows to create any number of user profiles, each of them having a specified list of contacts and a defined action (accept/reject) for the calls and SMS from these contacts.

If a user profile is selected, the contacts from the black list are blocked in addition to the ones from the profile list.

Black List

You can add the contact, from which you would like to block calls and SMS, into the black list. Calls and messages from the black listed numbers are blocked in case the **Black list** filtering mode or any user profile is selected. Therefore, the calls and SMS are not filtered by black list only if **Accept all** filtering mode is selected.

Create black list

1. To create the black list, on the main screen of the program tap the filtering section and then select **Configure** on the **Choose profile** menu.
2. Tap the **Black list** tab.
3. Tap **Add** to add numbers to the black list. You can select numbers by the following ways:
   - Select numbers from the contact list
   - Select numbers from the call and SMS logs
   - Enter numbers and information on them manually

   To search contacts in the phone book as well as in the call and SMS logs, you can use the search option available on pressing the **Search** button. When selecting numbers to add to the black list you can select them by one or multiple at one time.

   To add the selected numbers to the list, tap **Add**.
4. For each contact added to the black list, one of the following actions can be selected:
   - **Block calls and SMS** – to block all incoming calls and messages from the contact.

- **Block only calls** – to block only calls from the contact. Messages from him will be accepted.
- **Block only SMS** – to block only messages from the contact. Calls from him will be accepted.

By default, the **Block calls and SMS** action is selected for each new contact. You can change it if necessary.

5. To edit the information on the contact from the black list, tap and hold or swipe it in the list, then tap **Edit**. Modify the information entered in the **Name** and **Number** fields. Tap **Save**.

Information on the contact added to the black list from the phone book and also on the private numbers cannot be modified.

6. To delete a number from the list, tap and hold or swipe it, then tap **Delete**.
7. You can also create a list of keywords to block the SMS containing these words. To do this, in the adding contacts menu select the **Keyword** option. On the **Block SMS by keywords** screen enter the keyword and tap **Add**.

Clear black list

To delete all contacts from the black list, press the **Menu** button and select **Clear the list**.

Create Filtering Profile

Dr.Web anti-virus allows to create user profiles for the calls and SMS filtering.

Create a new profile

1. In the list of available profiles tap **Configure**.
2. On the **Profiles** tab tap **Add profile**.
3. Enter the profile name.
4. Specify an action for all incoming calls and messages from the profile list numbers. You can select one of the following actions:
   - **Allow only contacts from the list** – to accept the calls and SMS only from the contacts included into the current profile list
   - **Block contacts from the list** – to block calls and SMS from the contacts of current profile
5. Tap **Add number** to add contacts into the list. You can select numbers by the following ways:
   - Select numbers from the contact list
   - Select numbers from the calls and SMS logs
   - Enter numbers and information on them manually.

   To search contacts in the phone book as well as in the call and SMS logs, you can use the search option available on pressing the **Search** button. When selecting numbers to add to the list you can select them by one or several at one time.

   To add the selected numbers to the list, tap **Add**. The number on contacts in the profile list is displayed in parentheses to the right of the profile name.

The list of contacts of the user profile cannot be empty.

6. To edit the information on the contact in the list, tap and hold or swipe it, then tap **Edit**. Modify the information entered in the **Name** and **Number** fields. Tap **Save**.

Information on the contact added to the black list from the phone book and also on the private numbers cannot be modified.

7. To delete a contact from the profile list, tap and hold or swipe it to make appear a menu, where tap **Delete**.

Contacts deleted from the user profile are not deleted from the phone book.

View Blocked Calls and SMS

The filtering section on the main screen of the program contains the information on the number of blocked calls and messages. To review the lists of the blocked calls and messages, tap the corresponding icon:

- – to open the list of the blocked calls
- – to open the list of the blocked messages

To the right on the header of each list the number of not viewed calls/messages is displayed in parentheses. For each call/SMS in th list the following information is displayed:

- Date and time of the call/SMS
- Number and name of the call/message sender

Actions for the blocked calls and messages

1. You can call the number of the blocked call. To do this, tap a call in the list. The screen with an entered number will open. To make a call, tap **Call**.
2. By tapping an SMS in the list you can review the message text and details and also select an action to perform on it:
   - **Restore** – to restore the SMS in the incoming messages list
   - **Delete** – to delete the SMS

Update

Dr.Web anti-virus uses **Dr.Web virus databases** to detect threats. These databases contain details and signatures for all viruses and malicious programs for mobile devices known at the moment of the application release. However modern computer viruses are characterized by the evolvement and modification; also new viruses sometimes emerge. Therefore, to mitigate the risk of infection, **Doctor Web** provides you with periodical updates to virus databases via Internet.

On the main screen of the program the date of the last update is displayed on the section **Update**.

Start update

1. To update virus databases tap the update section on the main screen.
2. Updating procedure will launch automatically.

It is recommended to update the virus databases on program installation to let **Dr.Web anti-virus** use the most recent information about known threats. As soon as experts of the **Doctor Web Anti-Virus Laboratory** discover new threats, the update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour.

Configure updates

By default, the updates are automatically downloaded four times a day. On the **Update** section of the settings screen (see Figure 6), you can enable/disable the use of mobile networks to download updates. Select the **Do not use mobile networks** check box to disable the use of the mobile networks to download the updates. If no Wi-Fi networks is available, you will be offered to use 3G or GPRS. Changing this setting does not affect the use of mobile networks by other application and device functions.

Updates are downloaded via Internet. You may be additionally charged by your mobile operator for the data transfer. For detailed information, contact your mobile operator.

Quarantine

Dr.Web anti-virus allows you to move the detected threats to quarantine, where they are isolated from the rest of file system and therefore cannot damage the system.

Manage files in quarantine

1. To review the list of the threats moved to quarantine, open the application menu on the main screen and then tap **Quarantine**.
2. The list of all threats in quarantine will open (see Figure 9).
3. Tapping the threat in the list brings you to the window with the following information on the threat:
   - File name
   - Path to the file
   - Date of moving to quarantine

   You can also open the link on the **Information on the web** section to read the detailed information on the threat on **Doctor Web** official web-site.
4. For each threat in the list one of the following action can be performed:
   - **Restore** – to return the file back to the folder where it was moved from (use this action only if you are sure that the file is safe);
   - **Delete** – to completely remove the file from the device.
   - **Report false positive** – to send the file to **Doctor Web Anti-Virus Laboratory** and report that it does not contain any threats and was identified as suspicious by mistake. Enter your email in order to receive the results of the file analysis. Then tap **Send**.

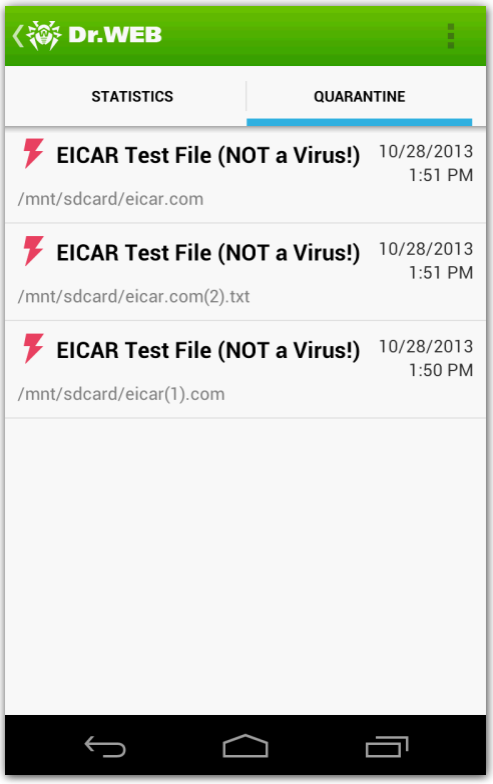


Figure 9. Quarantine

Quarantine size

You can review the information on the memory occupied by quarantine and the SD card free space. To do this, open the application menu on the **Quarantine** tab and select **Quarantine size**.

Statistics

Dr.Web anti-virus compiles the statistics of detected threats and program actions. To view the statistics, on the main screen open the application menu and then tap **Statistics**.

The **Statistics** tab contains two following information sections (see Figure 10):

- **Total** section contains the information on the total number of scanned files, detected and neutralized threats.
- **Actions** section contains the information on scanner start/stop, monitor enable/disable, detected threats and performed actions of the program.

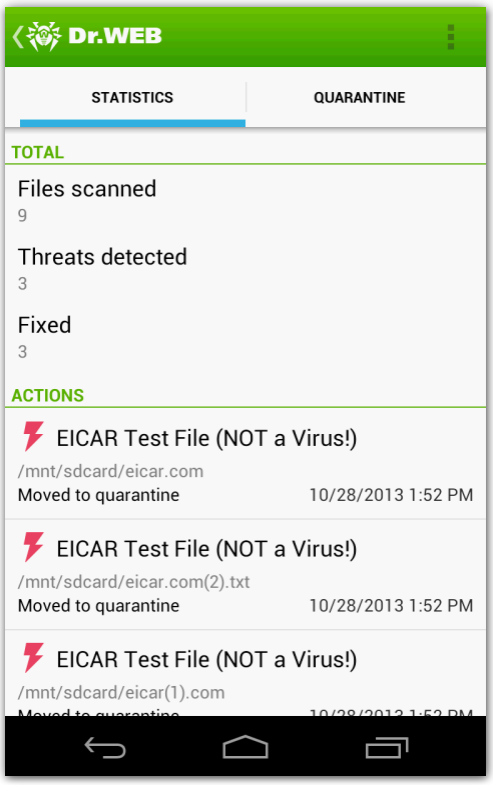


Figure 10. Statistics

Clear statistics

To clear all the statistics, open the application menu on the **Statistics** tab and tap **Clear statistics**.

Event log

Dr.Web anti-virus logs the events related to its operation in a special file that can be saved on SD card for further sending to **Doctor Web** Technical Support in case you experience troubles while using **Dr.Web anti-virus**.

To save the event log:

1. Open the application menu on the **Statistics** tab and then tap **Save log on SD card**.
2. The log will be saved in DrWeb_Log.txt file located in the Android/data/com.drweb/files folder on SD card.

Dr.Web Anti-theft

Dr.Web Anti-theft allows to detect the device location or lock its functions in case it has been lost or stolen.

You can manage **Dr.Web Anti-theft** using special SMS commands. To access the **Dr.Web Anti-theft** configuration parameters, you need to enter a special password set during the initial configuration. Be careful to remember this password as it is used to manage all the functions of **Dr.Web Anti-theft** and also to unlock your device in case it is locked. If you forgot your password set for **Dr.Web Anti-theft**, you can use the special service to reset the password and to unlock your device.

Dr.Web Anti-theft also allows to create a Buddies list (up to 5 phone numbers) to send SMS commands to your device even if you forgot your password for **Dr.Web Anti-theft**.

Configure General Settings

On the first start of **Dr.Web Anti-theft** a wizard window opens to help you to set you the main functions of the component:

- Tap **Continue** to set up the main functions of **Dr.Web Anti-theft**.
- Tap **Cancel**, if you want to configure **Dr.Web Anti-theft** later.

Configuring general settings of Dr.Web Anti-theft using the Wizard

1. On the first step of setting up **Dr.Web Anti-theft** enter a password. Your password should contain at least 4 characters. You will need to enter this password to manage all functions of **Dr.Web Anti-theft**. You can make the characters visible when entering the password by tapping to the right of the password field. To hide the entered password, tap . Tap **Next**.
2. Confirm the entered password. Tap **OK**.
3. Configure the Buddies list. Tap **Next**.
4. If you do not have a Google account, you will be asked to enter an email address to register **Dr.Web Anti-theft** on the **Doctor Web** server. It is required for sending you the special code to unlock your device or set a new password in case you forget the password set for **Dr.Web Anti-theft**. Provide an existing email address and tap **Continue**.

A working Internet connection is required for registering the email address on the server.

5. Enter the text which will be displayed on the screen of the locked device. Tap **Continue**.
6. This completes the general configuration of **Dr.Web Anti-theft**. You will be then asked to register the email address of your Google account (or the one specified on the previous step) on the **Doctor Web** server. Tap **Finish** to start the registration procedure:
   - if the registration completes successfully, the Wizard window closes and the **Dr.Web Anti-theft** settings screen (see Figure 11) opens.
   - in case an error occurs during the registration, its description is displayed on the screen and **Dr.Web Anti-theft** is not activated on your device.

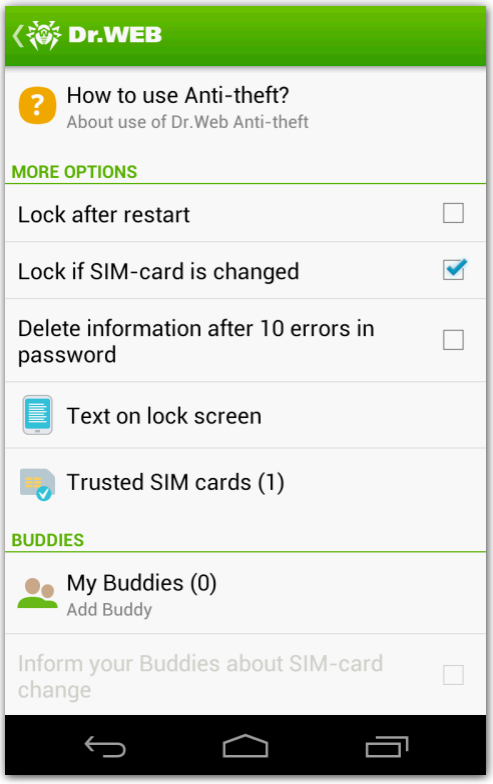


Figure 11. Dr.Web Anti-theft settings

Before opening the settings screen of **Dr.Web Anti-theft**, you will see a prompt to grant **Dr.Web anti-virus** the device administrator privileges, that you need to accept for correct operation of **Dr.Web Anti-theft**.

Getting help

To open the help on **Dr.Web Anti-theft**, on the **Dr.Web Anti-theft** settings screen (see Figure 11), tap **How to use Anti-theft?** on the **Help** section.

Changing password

To change the password set for **Dr.Web Anti-theft**, on the **Dr.Web Anti-theft** settings screen (see Figure 11) screen perform the following actions:

1. On the **Password and administration** section tap **Change password**.
2. Enter your current password. Tap **OK**.
3. Enter a new password. Tap **Continue**.
4. Confirm your new password. Tap **OK**.

Registering new email address

To change the email address registered for **Dr.Web Anti-theft** on the **Doctor Web** server, on the **Dr.Web Anti-theft** settings screen (see Figure 11) perform the following actions:

1. On the **Password and administration** section tap **Change e-mail**.
2. Enter the email address to register on the **Doctor Web** server. Tap **OK**.
3. A confirmation of the email address change will be sent to the previous email address.

Disabling Dr.Web Anti-theft

To disable **Dr.Web Anti-theft** on your device, on the **Dr.Web Anti-theft** settings screen(see Figure 11) perform the following actions:

1. On the **Password and administration** section tap **Disable Dr.Web Anti-theft**.
2. Enter the password set for **Dr.Web Anti-theft** and tap **Disable Dr.Web Anti-theft**.

Disabling **Dr.Web Anti-theft** significantly decreases the protection level of your device!

Additional Functions

To configure **Dr.Web Anti-theft**, on the main application screen tap **Anti-theft**. To access to the **Dr.Web Anti-theft** settings screen (see Figure 11) , enter the password set for the **Dr.Web Anti-theft** on its first start. If you forgot your password, send and SMS with the **#RESETPASSWORD#** command to your device from the number included into the Buddies list or use a special service.

Additional settings

To configure **Dr.Web Anti-theft**, on the **Dr.Web Anti-theft** settings screen (see Figure 11), perform the following actions on the **More options** section:

- To lock your device after it is restarted, enable the **Lock after restart** option.
- To lock your device in case the SIM card is changed, enable the **Lock if SIM-card is changed** option.
- To completely delete all your personal data from the SD card after 10 errors in entering password, enable the **Delete information after 10 errors in password** option.
- To specify the text which is displayed on the screen of the locked device, tap **Text on lock screen**, enter the text (e.g., you can add your contact information to return you the lost device), then tap **Save**.
- To review and edit the list of trusted SIM cards, tap **Trusted SIM cards**.

Trusted SIM cards

You can add the SIM cards that you use with your mobile device in a special trusted SIM cards list of **Dr.Web Anti-theft**. When you change one trusted SIM card to another one from the list, your device won't be locked by **Dr.Web Anti-theft**. The trusted SIM cards can be added at the device reboot or when opening **Dr.Web anti-virus**. You can also add the no SIM mode to the trusted list.

The no SIM mode is active either when the SIM card is missing physically or in case the installed applications have no access to the information about the SIM cards on the device. As a result, you can get an erroneous message about the SIM card missing, but if you make the no SIM mode trusted, all **Dr.Web Anti-theft** functions will be fully available.

To view or edit the list of trusted SIM cards, tap **Trusted SIM cards** in the additional settings of **Dr.Web Anti-theft**:

1. By default, the added SIM cards are named SIM1, SIM2, etc. To rename a SIM card, tap it in the list (or press and hold it, then tap **Edit** in the menu). In the SIM card information window, enter the new name into the **Name** field and tap **Save**.
2. To delete a SIM card from the trusted list, press and hold it, then tap **Delete** in the menu.

The SIM card that is currently in use on your device cannot be deleted from the list.

Buddies List

Dr.Web Anti-theft allows to add up to 5 phone numbers to the Buddies list. You can specify sending SMS commands without entering password for these numbers. You can also send an SMS command to disable **Dr.Web Anti-theft** and reset its password from these numbers.

Create Buddies list

1. On the **Dr.Web Anti-theft** settings screen (see Figure 11), tap **My Buddies** on the **Buddies** section.
2. Tap **Add** to add numbers to the Buddies list. You can select numbers by the following ways:
   - Select numbers from the contact list
   - Select numbers from the call and SMS logs
   - Enter numbers and information on them manually

   To search contacts in the phone book as well as in the call and SMS logs, you can use the search option available on pressing the **Search** button. When selecting numbers to add to the Buddies list, you can select them by one or multiple at one time.

   To add the selected numbers to the list, tap **Add**.
3. To edit the information on the contact from the Buddies list, tap it in the list and then modify the information entered in the **Name** and **Number** fields. Tap **Save**.
4. To delete a number from the Buddies list, tap and hold it, then tap **Delete**.
5. To notify your Buddies about changing the SIM-card in your device, enable the **Inform your Buddies about SIM card change**.
6. To allow sending SMS commands from the Buddies numbers without entering the **Dr.Web Anti-theft** password, enable the **Allow SMS commands without password** option.

Even if the **Allow SMS commands without password** option is disabled, your Buddies can send you the **#RESETPASSWORD#** command without password. This command is used to unlock the device and to reset the password for **Dr.Web Anti-theft**.

SMS Commands

You can manage **Dr.Web Anti-theft** by sending special SMS commands, which allow getting information on your device location or lock its functions and delete your personal data.

SMS commands table

You can use the following SMS commands to manage **Dr.Web Anti-theft**:

Command	Action
#SIGNAL#*Password#*	Lock the device and enable a sound alert which remains active even after restarting the device.
#LOCK#*Password#*	Lock the device.
#UNLOCK#*Password#*	Unlock the device without resetting the **Dr.Web Anti-theft** password.
#LOCATE#*Password#*	Get the GPS coordinates of the device in an SMS. This SMS contains a link indicating the device location on the map. After you tap the link, the device location is indicated by a special **Doctor Web** service called **Dr.Web Anti-theft Locator**. It opens a map in the Internet browser window and locates the device on it. The exactitude of the device coordinates depends on GPS receiver availability, Wi-Fi networks and GSM transmitting stations visibility. Thus, depending on the available data, the received coordinates may be exact (displaying a position on the map) or approximate (displaying a circle of a certain radius). You can select a map service from the list at the top of the map page.
#WIPE#*Password#*	Restore the factory settings of the device and delete all the information on the SD-card. This action will be also performed in case of 10 error when entering the password and the **Delete information after 10 errors in password** option is enabled in the **Dr.Web Anti-theft** settings.
#RESETPASSWORD#	Unlock the device and reset the **Dr.Web Anti-theft** password. This command can be sent only from the number included into the Buddies list.

SMS commands are not case sensitive. For example, to lock the device, you can send the **#LOCK#***Password#* command written as **#Lock#***Password#*, **#lock#***Password#*, **#lOck#***Password#*, etc.

To get more precise results after sending the #LOCATE# command, enable the use of the mobile networks for geolocation in the device parameters.

To send SMS command via Dr.Web Anti-theft interface

You can send SMS commands directly from **Dr.Web Anti-theft** interface to the devices on which **Dr.Web Anti-theft** resides. Do the following:

1. On the **Dr.Web - Anti-theft** screen (see Figure 11), tap **Send SMS command** on the **Buddies** section.
2. Enter the phone number to send the SMS command to.
3. Select a command from the list:
   - **Lock phone** – corresponds to the #LOCK# command.
   - **Lock phone and enable sound alert** – corresponds to the #SIGNAL# command.
   - **Unlock phone** – corresponds to the #UNLOCK# command.
   - **Delete all data** – corresponds to the #WIPE# command.

- **Detect phone location** – corresponds to the #LOCATE# command.
- **Reset password** – corresponds to the #RESETPASSWORD# command.

4. Enter the password, set for **Dr.Web Anti-theft** on the command recipient device. If you are in the Buddies list of the command recipient, you don't need to enter the password.
5. Tap **Send**.

Unlock the Device and Reset Password

If you forgot your password set for **Dr.Web Anti-theft** and you device is locked, perform the following actions:

1. Open the **Dr.Web Anti-Theft Unlock Code Request System** page at https://antitheft.drweb.com/.
2. Enter the code displayed on the screen of the locked device and the email you used to register **Dr.Web Anti-theft** on the **Doctor Web** server into the corresponding fields.
3. Click **Send code**. A special code to unlock the device and disable **Dr.Web Anti-theft** will be sent to the specified email address. Enter this code in the password filed on the screen of the locked device. This will disable **Dr.Web Anti-theft** on the device. To start using the **Dr.Web Anti-theft** function again, you need to re-enable and reconfigure it.

Restricting Internet Access

The access to the Internet ressources is controlled by the URL filter **Cloud Checker**. It allows to protect user of the mobile device from unsolicited Internet sites.

Cloud Checker can be used only to control the Internet ressources accessed via the default Android browser, Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser or Boat Browser Mini.

Cloud Checker allows to block access to the following categories of not recommended and potentially dangerous websites:

- Chats
- Drugs
- E-mail
- Gambling
- Known sources of virus
- Obscene language
- Social networks
- Terrorism
- Violence
- Weapon
- Adult content
- Not recommended sites.

To ensure that **Cloud Checker** works correctly, enable saving history function in your browser.

To enable/disable the URL filter

1. On the main application screen (see Figure 2), tap **Cloud Checker**. This will open the URL filter settings screen (see Figure 12).

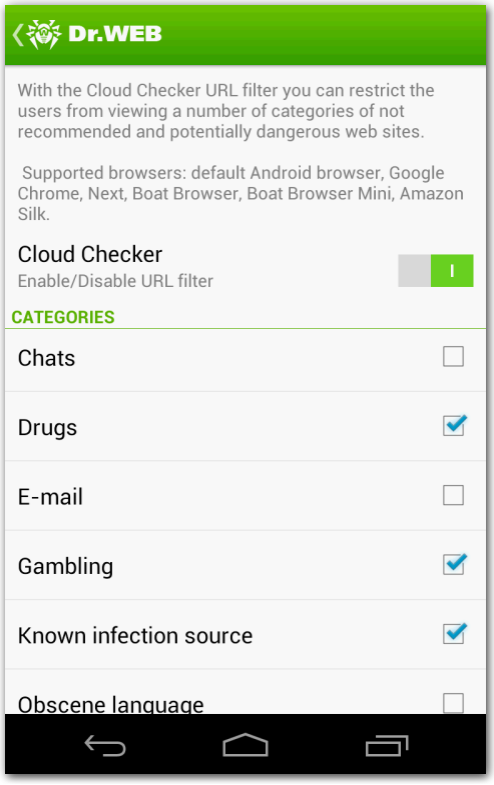

Dr.WEB
With the Cloud Checker URL filter you can restrict the users from viewing a number of categories of not recommended and potentially dangerous web sites.
Supported browsers: default Android browser, Google Chrome, Next, Boat Browser, Boat Browser Mini, Amazon Silk.
Cloud Checker
Enable/Disable URL filter
CATEGORIES
Chats
Drugs
E-mail
Gambling
Known infection source
Obscene language

Figure 12. The Cloud Checker settings screen

2. The URL filtering can be enabled/disabled using the **Cloud Checker** option. By default, The URL filtering is enabled.
3. In the **Categories** list, select the categories of the websites to block access to.

Dr.Web Firewall

Dr.Web Firewall protects your mobile device from unauthorized access and prevents leak of vital data through networks. This component monitors connection attempts and data transfer and helps you block unwanted or suspicious connections.

Dr.Web Firewall is based on VPN for Android technology. On some devices the protocol used by VPN may be disabled by manufacturer and is not available for non-system applications. In such cases the firewall functions are not available. For more information, please contact the manufacturer of your mobile device.

Enable/Disable Dr.Web Firewall

1. On the main application screen (see Figure 2) tap **Firewall**. The firewall configuration screen will open (see Figure 13).

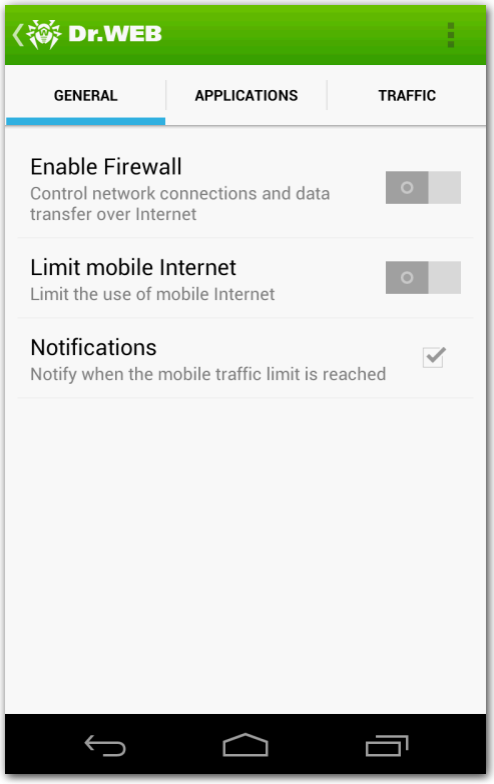


Figure 13. Firewall configuration screen. General tab

2. You can enable/disable firewall using the **Enable Firewall** option. By default, firewall is disabled. When you enable it, a dialog requesting to allow the use of VPN by **Dr.Web anti-virus** opens. To start using the firewall you need to give this permission.

If another application gets the rights to use VPN during **Dr.Web Firewall** operation, the component is disabled. The user is notified by a corresponding warning in the notifications section. To re-enable **Dr.Web Firewall**, tap this warning.

Features

Dr.Web Firewall is based on VPN for Android technology, so it does not require root access on the device. Therefore, **Dr.Web Firewall** can be used on any device running Android 4.0 or higher. However, using VPN for Android technology sets the following limits:

- At any moment of time, only one application installed on the device can use VPN. This results in opening a dialog requesting to allow using the VPN by this application. If the user gives such permission, the application starts using VPN, but it blocks access to VPN to another application that was using it just before the new request appeared. Such request appears when **Dr.Web Firewall** is enabled and every time the device is rebooted. It can also appear when other applications try to access VPN. VPN is shared between the applications in time, and the firewall is operating only when it gets full rights to use VPN.
- Another feature of VPN technology is related to possibility of **Dr.Web Firewall** to block only the connection with external networks (Internet). The connection within the local network cannot be blocked. This prevents the connections within the user home network from being blocked.

Dr.Web Firewall uses the VPN for Android technology only to perform its functions, without creating VPN tunnel, so the web traffic is not encrypted.

Limit the Use of Mobile Internet

Dr.Web Firewall allows you to limit the use of mobile Internet:

1. To enable/disable the limit for mobile Internet, use the **Limit mobile Internet** option on the **General** tab of the firewall configuration screen (see Figure 13).
2. Set up the limit for mobile traffic (in megabyte or gigabytes). You can select a duration period for the limit: a day, a week or a month.
3. If necessary, specify the amount of traffic that was already used since the selected limitation period has started:
   - If you selected a day as the limitation period, it begins at 00:00 of the current day.
   - If you selected a week as the limitation period, it begins at 00:00 of the current day.
   - If you selected a month as the limitation period, it begins at 00:00 of the first day of the current calendar month.

When the mobile Internet limit is enabled, a graph showing the amount of the remaining traffic appears on the **General** tab of the firewall configuration screen. The specified limit and the countdown to the limit expiration are shown next to the graph (see Figure 14).

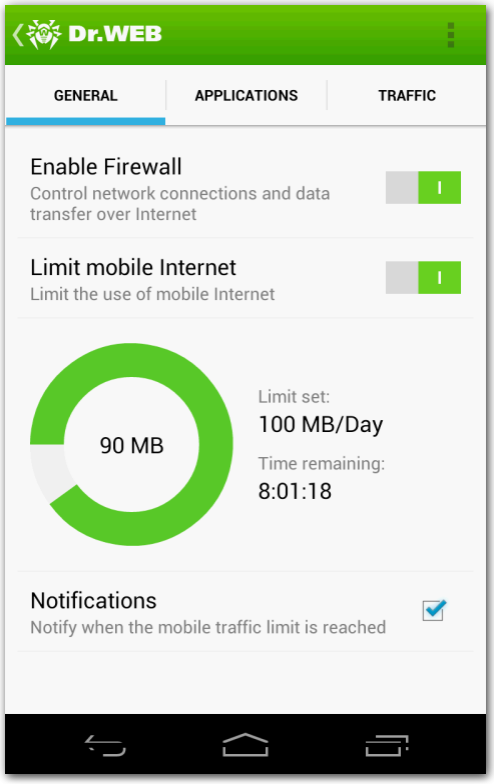


Figure 14. Firewall configuration screen with enabled mobile traffic limit

The specified mobile traffic limit may be overrun by up to 4 KB.

Notifications

You can set up notifications about reaching the mobile traffic limit by selecting the **Notifications** check box on the **General** tab of the firewall configuration screen (see Figure 13).

Processing Applications Traffic

Dr.Web Firewall allows to filter traffic on the application level and, therefore, control the access of applications to network resources. To view the information on the Internet traffic of applications installed on your mobile device, as well as to configure the connection rules for them, open the **Applications** tab of the firewall configuration screen (see Figure 15).

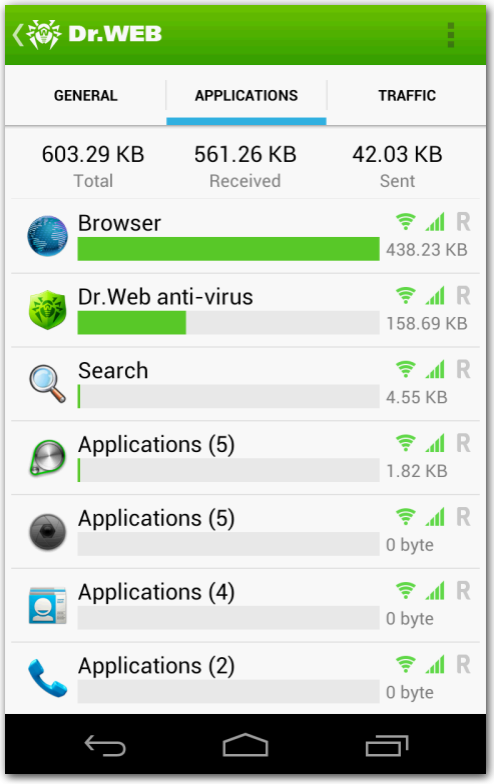


Figure 15. Firewall configuration screen. Applications tab

On the **Applications** tab, you can review the total amount of data transferred over the networks and the amount of sent and received data.

The **Applications** tab also features a list of applications (and application groups) with information on the traffic used by each of them. To open the list of all applications installed on your device, including those without any Internet traffic, select the **All applications** check box in the menu on the **Applications** tab.

You can enable/disable the use of Wi-Fi, mobile Internet and roaming for each application in the list using the corresponding options to the right of the applications names.

To review the detailed information on the use of Internet by an application (or an application group) from the list, tap it. On the application information screen, you can perform the following actions:

- Enable/disable the use of Wi-Fi, mobile Internet and roaming for this application (or application group).
- View the application log.
- View the Internet traffic statistics for this application (or application group).
- Configure connection rules for this application (or application group).

Internet Traffic Statistics

On the application (applications group) traffic screen, you can review the statistics of Internet traffic used by this application shown as a graph (see Figure 16).

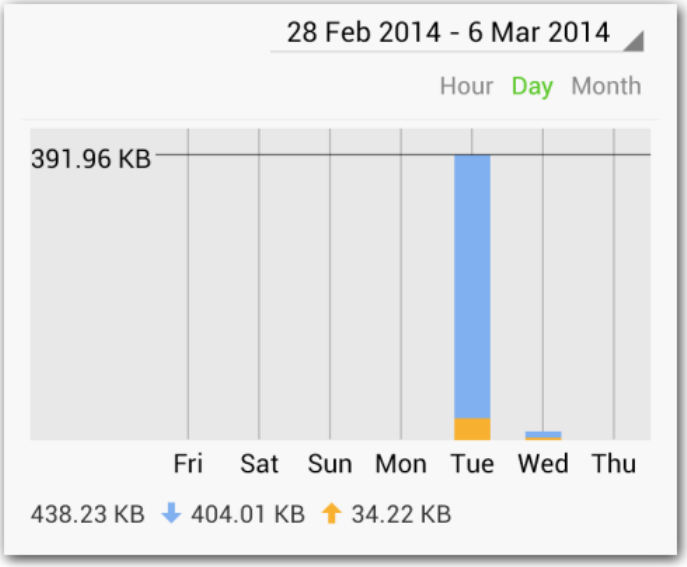


Figure 16. Application traffic statistics

The yellow color on the graph shows the outgoing application traffic, the blue one shows the incoming traffic. The numeric values of the application traffic amount (total, incoming and outgoing) are shown under the graph.

When reviewing the Internet traffic statistics, you can perform the following actions:

- Use the corresponding list to select the period to show statistics. You can review the statistics for the current day, last week, current month, previous month or specify any other period by selection the start and end dates.
- Configure showing the statistics for the hours, days or months within the selected period.

Clear statistics

If necessary, you can reset the whole firewall statistics or only the information for certain applications.

To delete the statistics for all applications:

1. On any tab of the firewall configuration screen (see Figure 13) open the menu and tap **Clear**.
2. On the **Clear log and statistics** window, select the **Clear statistics** check box and tap **OK**.

To delete the statistics for an application:

1. On the **Applications** tab of the firewall configuration screen (see Figure 15), select the application to delete the statistics for.
2. On the application information screen, open the menu and tap **Clear**.
3. On the **Clear log and statistics** window, select the **Clear statistics for this application** check box and tap **OK**.

Connection Rules

On the application (applications group) traffic screen, you can set up the rules for connections of this application to certain IP addresses and ports.

Configure rule sets

1. To create a new rule, tap **Add rule**. You can add allowing or blocking rules depending on the option selected in the **Connection rules** section:
   - If **Block connections from the list** is selected, you can add blocking rule.
   - If **Allow only the connections from the list** is selected, you can add allowing rule.
2. In the **New rule** window, fill in the **IP address** and **Port** fields. You can enter a valid IP address (in the a.b.c.d format), an IP addresses range (in the a1.b1.c1.d1-a2.b2.c2.d2 format) or a network (in the a.b.c.0/n format, where n is a number from 1 to 32) or leave the **IP address** field blank (in this case entering the port is obligatory). Enter the valid port in the **Port** field or leave it blank (in this case entering the IP address is obligatory). In case one of the fields is blank, the rule is valid for all the IP addresses or ports respectively. Tap **OK** to save the rule.
3. To edit an existing rule, tap and hold it, then tap **Edit**.
4. To delete a rule, tap and hold it, then tap **Delete**.

You can also add allowing and blocking rules when browsing the applications logs or the list of current Internet connections.

Incoming connections

The **Allow incoming** check box in th menu on the application information screen excludes the incoming connections from the firewall check. The information on the connections from any external addresses with the port opened by the application is only partially added to the application log and firewall statistics. Moreover, any connections with such addresses may be excluded from the processing by firewall for all other applications. Such operation mode is not safe and generally, it is not recommended to use it.

Allowing the incoming connections is useful in case the firewall cannot be disabled by other means, for example, when a server receiving connections from external networks is configured on the device.

Current Internet Activity

The **Traffic** tab of the firewall configuration screen (see Figure 13) contains information on current Internet connections initiated by applications installed on the mobile device. To open the detailed information on connections of a certain application (IP addresses and ports of the connections and the amount of the sent and received data), tap it in the list.

You can create allowing or blocking rules for connections from the list. Tap and hold the connection in the list, then tap the corresponding option:

- **Add allowing rule** to create a rule allowing the connections from the specified IP address and port for the selected application.
- **Add blocking rule** to create a rule blocking all the connections from the specified IP address and port for the selected application.

Logging

Dr.Web anti-virus logs the events related to the operation of **Dr.Web Firewall**. You can review the full log or the lists of events related to the use of Internet by separate applications.

Dr.Web Firewall Log

To open the list of all the events related to **Dr.Web Firewall** operation, open the menu and tap **Log** on any tab of the firewall configuration screen (see Figure 13).

View the log

To simplify searching the information when viewing the event log, use the sorting and fast scrolling (by moving a special graphical element in the right part of the screen) functions. To sort the records in the log, select the sorting criterion in the menu on the log screen.

You can review following information for each event in the log:

- Connection date and time (for TCP) or the time required to receive the packets with the corresponding traffic amount (for UDP). Example: 18/02/2014 2:07:11 - 18/02/2014 2:07:12.
- Local address and port. Example: src: 10.2.3.5:6881.
- Incoming and outgoing traffic (in bytes) or the number of blocked packets. Example: in:103 out:112 или blocked packets:1.
- ID of the application related to the traffic on the device (User ID). Example: uid=10071.
- Number of traffic jams (only for TCP). Example: traffic jam=0. Traffic jams are the special situations, when the client application struggles to unload all data from the TCP buffer, that results in "clogging", so the data transfer speed significantly decreases.

Clear log

To delete full log of **Dr.Web Firewall**:

1. On any tab of the firewall configuration screen (see Figure 13) open the menu and tap **Clear**.
2. On the **Clear log and statistics** window, select the **Clear log** check box and tap **OK**.

Log file size

By default, the maximum size for the log file is set to 5 MB. To change this value:

1. On any tab of the firewall configuration screen (see Figure 13) open the menu and tap **Clear**.
2. On the **Clear log and statistics** window enter the new value for the maximum log file size and tap **OK**.

Application Logs

To review the list of events related to the network connections of a certain application installed on your device, tap **Log** on the application information screen.

View the application log

All the events related to the application are grouped by date. To open the list of events for a certain date, tap it in the list. You can review the following information for each event:

- Connection time (for TCP) or the time required to receive the packets with the corresponding traffic amount (for UDP).
- Local address and port.
- Incoming and outgoing traffic (in bytes) or the number of blocked packets.

You can create allowing or blocking rules for connections from the application log. Tap and hold the connection in the list, then tap the corresponding option:

- **Add allowing rule** to create a rule allowing the connections from the specified IP address and port for the selected application.
- **Add blocking rule** to create a rule blocking all the connections from the specified IP address and port for the selected application.

Clear application log

To delete the log of an application:

1. On the application information screen, open the menu and tap **Clear**.
2. On the **Clear log and statistics** window, select the **Clear log for this application** check box and tap **OK**.

Disable logging for application

If necessary, you can disable logging for separate applications. To do this:

1. On the application information screen, open the menu and tap **Clear**.
2. On the **Clear log and statistics** window, select the **Disable logging for this application** check box and tap **OK**.

Security Troubleshooting

Dr.Web anti-virus performs diagnostics of the security of your device and helps resolving the detected problems and vulnerabilities using a special component - **Security Auditor**. This component is enabled automatically when the application is launched for the first time and after registering the license. The number of the detected problems is displayed on the **Security Auditor** section of the main application screen.

If no problems or vulnerabilities are detected by **Security Auditor** in the operation system of your device, the corresponding section is not displayed on the main application screen.

Resolving security problems

To review the list of the detected problems and vulnerabilities (see Figure 17), tap the **Security Auditor** section on the main application screen.

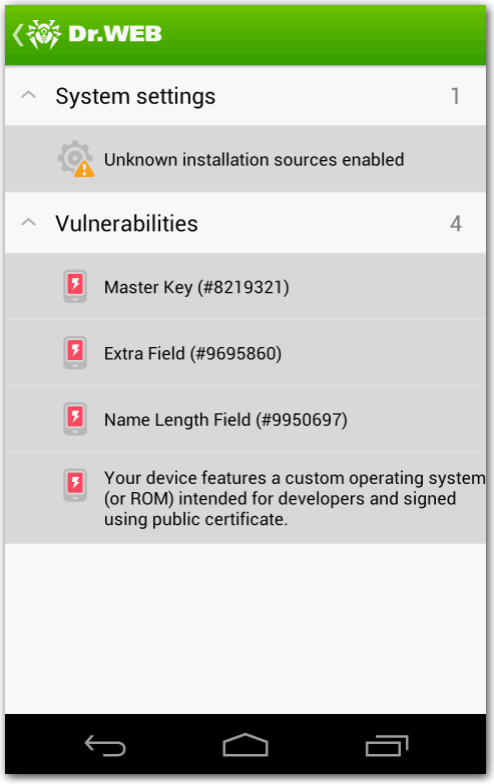

Dr.WEB
System settings 1
Unknown installation sources enabled
Vulnerabilities 4
Master Key (#8219321)
Extra Field (#9695860)
Name Length Field (#9950697)
Your device features a custom operating system (or ROM) intended for developers and signed using public certificate.

Figure 17. List of security problems detected on the device

Dr.Web anti-virus detects the following categories of security problems: applications with highest priority of SMS processing, hidden device administrators, vulnerabilities and system settings that affect the device security. To view the detailed information on any detected problem and to resolve it, open one of the categories and tap a problem in the list.

Applications with highest priority of SMS processing

This category contains the list of the applications installed on the device that have the higher priority in SMS processing than **Dr.Web anti-virus**. Such applications can block the operation of Dr.Web Anti-theft and SMS filtering, since they are first to process all incoming messages and commands. Sometimes such applications are malicious and may present a threat to the security of your device.

If you notice that the SMS filtering or **Dr.Web Anti-theft** does not work properly, try to change the priority settings of the applications in the list, if possible. These applications will disappear from the list of security problems. If you are not sure that these applications are totally safe, it is recommended to delete them from the device. To delete an application, tap **Delete** on the screen with the detailed information on the problem related to this application, or use the standard OS tools.

Hidden device administrators

Applications that are activated as device administrators but not shown on the list of administrators on the corresponding section of the device settings cannot be deleted by means of the operation system. Most likely, such applications are dangerous.

If you don't know why such application is not displayed in the list of device administrators, it is recommended to delete it from the device. To delete an application, tap **Delete** on the screen with the detailed information on the problem related to this application.

System settings

USB debugging and installing applications from unknown sources are the system settings that affect the security of the mobile device. It is insecure to use conflicting software as well:

- **USB debugging** is intended for developers and allows copying data from PC to the mobile device and vice-versa, installing the applications on the device, viewing their logs and deleting them in some cases. If you are not developer and do not use the debug mode, it is recommended to turn it off. To open the corresponding device settings section, tap **Settings** on the screen with detailed information on the problem.
- **Installing applications of unknown origin** is the main source of threats. Application downloaded from other source that official market (Google Play) are likely to be unsafe and present a threat to the mobile device security. To mitigate risks of installing the unsafe applications, it is recommended to disable installation of the programs from unknown sources. To open the corresponding device settings section, tap **Settings** on the screen with detailed information on the problem. It is also recommended to scan for viruses all the applications you install on your device. Make sure that **Dr.Web virus databases** are up to date before scanning.
- **Software conflicts**. Use of conflicting software, including web browsers that are not compatible with Cloud Checker URL filter, decreases the security level of your device, as it is not protected against the undesirable and malicious web resources. It is recommended to use and to assign as the default browser on your device one of the following browsers: the default Android browser, Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser or Boat Browser Mini.

Vulnerabilities

Dr.Web anti-virus detects such vulnerabilities as Master Key (#8219321), Extra Field (#9695860) and Name Length Field (#9950697) in the device system. They allow adding malicious code to some applications without changing their cryptographic signatures, that may result in acquisition of dangerous functions by these applications and damage the device. **Dr.Web anti-virus** also detects the Heartbleed vulnerability, that can be used by fraudsters to access the user confidential information.

If one or more of these vulnerabilities are detected on your device, check for operation system updates on the official website of your device manufacturer. Newer versions may have these vulnerabilities fixed. If there are no updates yet, it is recommended to install applications only from trusted sources.

The device may become vulnerable to different types of threats if it is rooted, i.e. the procedure of rooting has been performed to attain control (known as "root access") over the device system. It results in ability to modify and delete system files, that may potentially damage the device. If you rooted your device yourself, it is recommended to rollback the changes for security reasons. If root access is the integral feature of your device or you need it for your everyday tasks, be extremely cautious when installing applications from the unknown sources.

Operation Mode

If necessary, you can use **Dr.Web anti-virus** installed from the **Doctor Web** website to connect to corporate networks managed by **Dr.Web Control Center** or to access **Dr.Web® AV-Desk** anti-virus service of your IT provider. To operate in such central protection mode, you do not need to install additional software or uninstall **Dr.Web anti-virus**.

Operation in central protection mode is not supported by the version of **Dr.Web anti-virus** installed from Google Play.

To use central protection mode

1. Contact an anti-virus network administrator of your company or IT provider for parameters of connection to the central protection server.
2. On the main screen, open the application menu and select **Settings**.
3. To connect to the central protection server of your company or IT provider, on the settings screen (see Figure 6) select the **Dr.Web Agent** check box on the **Mode** section.

   In the central protection mode, the option of manual start and configuring updates is blocked. Some features and settings of **Dr.Web anti-virus**, particularly concerning the constant protection and on-demand scanning, may be modified and blocked for compliance with the company security policy or according to the list of purchased services. A key file for operation in this mode is received from central protection server. Your personal key file is not used. When the license is expired or blocked, contact your company or IT provider anti-virus network administrator in order to obtain a new license, after receiving the corresponding notification.

4. On switching to the central protection mode **Dr.Web anti-virus** restores parameters of the previous connection. If you are connecting to the server for the first time or connection parameters have changed, do the following:
   - Enter the IP address of the central protection server provided by administrator of anti-virus network.
   - Enter the authentification parameters: ID, which is assigned to your mobile device for registration at the server, and password. The entered values are saved and you need not enter them again when reconnecting to the server. To connect as a new station ("Newbie"), open the application manu and tap **Connect as "Newbie" station**.
   - Tap **Connect**.

The install.cfg file provided by administrator of anti-virus network contains settings to connect to the central protection server. To use this file, place it in any of the folders at the first nesting level on the SD card. If the file is downloaded to the device, fields for entering the connection settings will be filled in automatically.

If necessary, e.g., when the connection parameters have changed, you can reset the saved parameters. To do this, open the application menu on the connection settings entering screen and tap **Reset connection settings**.

If the connection failed and the error with **Unsupported option in server settings. Check server configuration and make sure that "Encryption" and "Compression" parameters are not set to "Yes".** description is returned, contact the anti-virus network administrator to resolve the problem. If you are the anti-virus network administrator, check the server settings and try to reconnect.

To use standalone mode

1. On the main screen, open the application menu and select **Settings**.
2. To switch to the standalone mode, clear the **Dr.Web Agent** check box on the **Mode** section of the settings screen (see Figure 6).

   On switching to this mode, all settings of **Dr.Web anti-virus** are unlocked and restored to their previous or default values. You can once again access all features of anti-virus.

3. For correct operation in standalone mode **Dr.Web anti-virus** requires a valid personal key file. The key files received from central protection server cannot be used in this mode. If necessary, you can receive or update a personal key file with License Manager.

To configure the available applications list

If you are the administrator of the anti-virus network, you can specify the list of applications available for the users on their devices. To do this:

1. On the main screen of the application tap **Administrator**.
2. Select the applications, which will be available for the anti-virus network users on their mobile devices.
3. Tap **Allow selected**.

URL Shortening Service

Sometimes, for example, when you have to deal with limits on the number of characters in SMS or social networks posts, you may need to use short URLs. **Dr.Web anti-virus** allows shortening the URLs and scanning them for viruses using a special link shortening service in order to protect users from security threats.

Using URL shortening service

To check and shorten the URL:

1. Select the URL you want to check and shorten, then use the sharing function of your browser.
2. In the menu that opens, tap **Shorten URL**. The page that the selected URL links to will be scanned for threats and, if it is safe, the shortened URL will be created and copied to clipboard. If the page contains security threats, the service will show the corresponding notification.

Appendices

Appendix A. Technical Support

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/doc/
- Read the frequently asked questions at http://support.drweb.com/show_faq/
- Browse the **Dr.Web** official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-form in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, see the **Doctor Web** official website at http://company.drweb.com/contacts/moscow.

Index

A

anti-spam 25
anti-virus network 47
anti-virus protection 21
applications
  connection rules 42
  incoming connections 42
  statistics 42
  traffic 42
autorun files 21, 22

B

black list 26

C

central protection 47
Cloud Checker 37
  settings 37
  supported browsers 37
  web sites categories 37
connection rules 42
constant protection 21
custom scan 22

D

demo key file 9
device lockers 25
document conventions 6
Dr.Web Anti-theft 32
  buddies list 35
  disable 32, 37
  password 32
  registration 32
  reset password 37
  settings 32, 34
  SMS commands 36
  trusted SIM cards 34
  wizard 32
Dr.Web Anti-theft Locator 36
Dr.Web anti-virus 6
  actions 24
  anti-spam 25
  anti-virus protection 21
  black list 26
  Cloud Checker 37
  Dr.Web Anti-theft 32, 34, 35, 36, 37
  Dr.Web Anti-theft Locator 36
  Dr.Web Firewall 38
  export settings 20
  filtering 25, 26, 28
  filtering profiles 27
  functions 20
  import settings 20
  install 13
  interface 16
  key file 8
  launch 16
  license 8
  log 31
  main features 7
  monitor 21
  My Dr.Web 19
  notifications 18
  operation mode 47
  quarantine 29
  reset settings 20
  scanner 22
  security troubleshooting 45
  settings 20
  SpIDer Guard 21
  start to use 16
  statistics 31
  system requirements 13
  technical support 50
  uninstall 13, 14
  update 28
  URL shortening 49
  widgets 18
Dr.Web Firewall 38
  applications traffic 41, 42
  incoming connections 42
  Internet traffic 43
  limit mobile Internet 40
  logging 43, 44
  network connections 43

E

export settings 20

F

false detection 22, 24, 29

Index

false positive 22, 24, 29
filtering 25
  black list 26
  calls 25
  messages 25
  mode 26
  profiles 27
  view blocked 28
filtering mode 26
filtering profiles 27
filters 26
  black list 26
  user 27
full scan 22

G

Google Play 13, 14

H

hidden device administrators 45

I

import settings 20
install program 13
interface 16
Internet traffic
  applications 41, 42
  mobile 40

K

key file 9
  acquire 9
  copy from file 10
  download 9
  update 12
  use 10
  validity 9

L

launch program 16
license
  acquire 9
  copy from file 10
  download 9
  purchase 9
  register serial number 10
  renew 12
  update 12
  use 10
  validity 9
license key file 9
licensing 8
log 31
  applications 44
  Dr.Web Firewall 43
logging 31

M

main features 7
market 13, 14
mobile Internet
  limit 40
  notifications 40
monitor
  enable 21
  settings 21
  statistics 21
My Dr.Web personal page 19

N

network connections
  current activity 43
notifications 18
  license 12
  mobile Internet 40
notifications pane 18

O

ongoing notifications 21
operation mode 47

P

processing threats 24, 25, 29
  quarantine 24
  sounds 24
protection status 16
purchase license 9

Q

quarantine
  processing threats 29
  size 29

Index

quick scan 22

R

ransomware 25
register serial number 10
reset settings 20
root access 45
rooting 45

S

scan
- custom 22
- full 22
- quick 22

scanner
- custom scan 22
- full scan 22
- quick scan 22
- settings 22
- statistics 22

security troubleshooting
- hidden device administrators 45
- incompatibility 45
- root access 45
- sms processing priority 45
- software conflicts 45
- system settings 45
- vulnerabilities 45

send file to laboratory 22, 24, 29
settings
- Dr.Web Anti-theft 32, 34
- export 20
- import 20
- monitor 21
- reset 20
- scanner 22
- update 28
- URL filter 37

sms processing priority 45
software conflicts 45
SpIDer Guard
- enable 21
- settings 21
- statistics 21

start to use 16
statistics 31
- applications traffic 42
- monitor 21
- scanner 22

support 50
supported browsers 37
system requirements 13
system settings 45

T

technical support 50
threats
- actions 24
- device lockers 25
- system applications 24

trusted SIM cards 34

U

uninstall program 13, 14
update
- automatic 28
- settings 28

URL filter 37
URL shortening 49

V

view blocked 28
virus databases
- automatic 28
- update 28

vulnerabilities 45

W

widgets 18

© Doctor Web, 2014